February 2005

Operator's Lesson Plan

I. IDACS Coordinator Duties and Responsibilities

A. The agency head appoints the IDACS Coordinator by notifying IDACS in writing.

B. The following are terminal coordinator responsibilities as listed in the Indiana Administrative Code (IAC).
240 IAC 5-2-8 Terminal agency operations; coordinator; duties and responsibilities.
Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 10-4-1-6-7; IC 10-1-2.5-3

Sec. 8. Once operational on the IDACS System, each terminal agency is required to designate one (1) individual as coordinator to serve as liaison between that department and the IDACS committee. It is important that the person selected becomes familiar with all phases of IDACS to efficiently carry out all duties and responsibilities assigned. Duties and responsibilities are as follows:

1. All agency personnel, including any non-terminal agencies serviced, utilizing system information are aware of the rules and policies of the IDACS/NCIC/NLETS system.

2. Disseminate the contents of the IDACS/NCIC newsletters to all terminal operators and non-terminal agencies serviced.
   a. The intent of the newsletter is to keep users informed.

3. Validation reports are properly processed.

4. Terminal operators receive proper IDACS training in accordance with the IDACS certification-training program.

5. Inform IDACS of any changes in the agency head, coordinator, agency address, or terminal site.

6. Report all IDACS rules violations and other improper uses to IDACS.

II. System Officials and Organization

A. The following are IDACS Committee Rules as listed in the Indiana Administrative Code (IAC).

240 IAC 5-1-1 General policy: restrictions on use
Authority: IC 10-1-1-3; IC10-1-2.5-7
Affected: IC 10-1-2.5-2

Sec. 1. (a) A committee appointed by the Superintendent of the Indiana State Police, for the purpose of managing and controlling the Indiana Data and Communications System hereinafter called "IDACS", has the responsibility for the management of the statewide system network as imposed by these rules and as directed by the Superintendent of the State Police. The committee chairman shall be selected by the Superintendent. The chairman shall report activities of the committee to the Superintendent for review and approval.
To make sure the proper operation of the systems, the standards, procedures, formats, and criteria as set forth herein shall be strictly adhered to. In this respect, as in system security, the IDACS terminal agency shall not only follow the rules set forth, but shall also ensure that agencies they are servicing do the same.

B. IDACS Committee Membership

1. The IDACS Committee is composed of several voting members, a chairman, and a number of non-voting members appointed by the State Police Superintendent.

2. Voting members of the committee are as follows:

   a. Chairman (votes only in a tie situation)
   b. Indiana Sheriff's Association
   c. Indiana Chiefs of Police Association
   d. State Police Records Division
   e. State Police Communications Division
   f. State Police Criminal Justice Data Division
   g. State Police IDACS Section
   h. State Police Systems & Programming
   i. IDACS Area I Representative
   j. IDACS Area II Representative
   k. IDACS Area III Representative
   l. IDACS Area IV Representative
   m. IDACS Area V Representative

3. Non-Voting members of the committee:

   a. IDACS Security Officers
   b. Data Operations Section
   c. Fiscal Division
   d. Legal Advisor

4. IDACS Committee meetings are held once every quarter normally on the first Tuesday of the following months: March, June, September, and December.

a. The meeting is open to all interested persons.

5. Area Representatives

a. Area Representatives will be nominated every two (2) years by the Area they are to represent.
b. Nominees shall be either the IDACS Coordinator or in a management position for an IDACS Terminal Agency.
c. The nominee must be approved by the State Police Superintendent.
d. Represents his/her Area on the IDACS Committee.
e. Area Meetings
1. Must have at least one (1) Area meeting during each half of the calendar year.
2. The meeting is opened to all IDACS Coordinator's in the Area.
3. The meeting is designed to inform Area Representatives of the IDACS Coordinator's concerns and suggestions for input to the IDACS Committee. It is also designed for Area Representatives to inform IDACS Coordinator's of the work being conducted by IDACS.

III. Terminal Agency User Agreements and Security

A. The following is information concerning terminal agency user agreements and system security as listed in the Indiana Administrative Code (IAC).

240 IAC 5-2-9 User Agreement
Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 5-2-5; IC 10-1-2.5-4

Sec. 9. (a) All IDACS user agencies shall complete a "user agreement" before utilizing the system. Agencies with terminals and statutory police agencies shall complete such agreements with the Indiana State Police and the IDACS Committee. Non-terminal agencies shall complete an agreement with the terminal agency that services them. Agencies that only have mobile data devices (MDD's) and that have direct access to IDACS/NCIC, must sign a terminal agency user agreement with the Indiana State Police.

B. Purpose of Agreement

1. This agreement provides for the IDACS Committee to serve as the agency responsible for the exchange of statewide criminal offender record information and other criminal justice and law enforcement information between IDACS and the terminal agency. In addition, it provides for the Indiana State Police to serve as the State Control

Terminal agency to facilitate the interchange of wanted file/computerized criminal history record information between NCIC and the terminal agency and message switching functions between NLETS and the terminal agency, via the IDACS network.

C. Terminal/Non-Terminal Agency Agreements

1. This agreement provides for the IDACS terminal agency to serve as the agency responsible for the exchange of statewide criminal offender record information and other criminal justice and law enforcement information between IDACS and the non-terminal agency. In addition, it provides for the terminal agency to serve as the agency to facilitate the interchange of wanted file/computerized criminal history record information between NCIC and the non-terminal agency and message switching functions between NLETS and the non-terminal agency, via the IDACS network.

2. Those agencies that only have mobile data devices (MDD's) must sign a non-terminal agency user agreement with the terminal agency that services them (i.e. entries, validations, CHRI, III, etc.).

3. Each terminal agency must keep on file copies of the Terminal Agency User Agreement and any terminal/non-terminal agency agreements with the agencies they service. These agreements must be made available upon request of the IDACS Security Officer.

4. New agreements are required when the agency head changes.

D. Who May Access System Data

240 IACa 5-2-10 Security; confidentiality

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 10-1-2.5

Sec. 10. (a) "SYSTEM" as used in the security and confidentiality rules means IDACS, NLETS, and/or NCIC terminals, equipment and any and all data accessible from or stored therein.

1. Access, meaning the ability to obtain from the System, shall be permitted only to criminal justice agencies in the discharge of their official mandated responsibilities, and those agencies as required by state and/or federal enabling authority. Agencies that shall be permitted access to SYSTEM data include the following:

a. Police forces and departments at all governmental levels (including private college and railroad police departments as authorized by Indiana Code) that are responsible for enforcement of general criminal laws.

b. Prosecutive agencies and departments at all governmental levels.

c. Courts at all governmental levels with a criminal or equivalent jurisdiction.

d. Correction departments at all governmental levels, including corrective institutions and probation departments.

e. Parole commissions and agencies at all governmental levels.

f. Agencies at all governmental levels which have as a principle function the collection and provision of fingerprint identification information.

g. Regional or local governmental organizations established pursuant to statue which collect and process criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

h. Approved noncriminal justice agencies may have access to SYSTEM data on a limited basis. "Limited basis" means restricted to only that data recommended through resolution by the IDACS committee and approved by the State Police Superintendent.

E. Terminal Security Measures

1. All agencies and computer centers having devices on the SYSTEM and/or having access to SYSTEM data shall physically place these devices in a secure location previously approved by the IDACS Committee within the authorized agency. Subsequent physical location changes of devices shall have prior approval of the IDACS Committee.

a. A secure location is defined as: secure from public access and view of the screen and/or printed data.

F. Personnel Security Measures (Device Operators)

1. Since personnel at these computer centers have access to data stored in the SYSTEM, they shall be screened thoroughly under the authority and supervision of the IDACS committee or their designated representative.

2. This screening shall also apply to noncriminal justice maintenance or technical personnel. The screening process shall consist of a character investigations, including fingerprints, for the purpose of establishing suitability for the position. Investigations shall consist of the gathering of information as the applicant's honesty, integrity and general reputation. Personal characteristics or habits, such as lack of judgment, lack of physical or mental vigor, inability to cooperate with others, intemperance, or other characteristics which would tend to cause the applicant to be unsuitable for this type of position, shall be considered sufficient grounds for rejection. Convincing information in an applicant's past history involving moral turpitude, disrespect for law, or unethical dealings shall be considered sufficient grounds for rejection. If any of the above facts are presented to the IDACS committee, a recommendation shall be made and presented to the State Police Superintendent for a final approval or disapproval decision.

G. System Data Security

1. Audit requirements of SYSTEM data.

240 IAC 5-1-2 Audit of system transactions

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 10-1-2.5-3

Sec. 2. (a) Established IDACS committee policy requires all user agencies to Maintain an audit trail for six (6) months for certain types of IDACS transactions as itemized but not limited to the following:

1. Administrative Messages (AM) (both transmitted and received).

2. Bureau of motor vehicles and department of natural resources information file data.

3. IDACS/NCIC stolen file data.

4. Out-of-State (NELTS) Bureau of Motor Vehicles or Department of Natural Resources data.

a. These audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated. Audit trails shall be maintained manually or by automation, and shall be made available to the IDACS Committee for inspection upon request.

b. It should be noted that these are minimum requirements and it may be necessary to keep important or case related information for longer periods of time in order to properly confirm or validate IDACS/NCIC wanted entries.

5. Audit requirements for Criminal History Data

a. NCIC and IDACS require that an audit trail for the dissemination of criminal history be kept for one (1) year. This includes the Violent Gang and Terrorists Organization File (VGTOF) and Sexual Offender File (SOF).

240 IAC 5-1-3 Audit of Criminal History Record Dissemination

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 4-1-6; IC 10-1-2.5-3

Sec. 3. 28 U.S.C. states that audits shall be kept pertaining to the dissemination of criminal history records. This includes responses from NCIC's Interstate Identification Index (NCIC III) and responses from state central repositories and other agency criminal history files (both in-state and out-of-state). Such audit records shall include, but are not limited to, the names of all persons or agencies to whom the information is disseminated and the date and time upon which such information is disseminated.

b. The Violent Gang and Terrorists Organization File is in NCIC only. The information in the VGTOF file is provided in the "Hot" file format. NCIC's and IDACS policy is to treat the VGTOF file as Criminal History.

6. IDACS is primarily a system for law enforcement/criminal justice users and as such only data related to law enforcement/criminal justice shall be transacted by the system. Information furnished through the system shall be restricted to the use of authorized law enforcement/criminal justice agencies, or those authorized noncriminal justice agencies performing criminal justice responsibilities, and shall not be sold, transmitted, or disseminated to any noncriminal justice agency or person unless authorized by the State Police Superintendent.

Such authorization for dissemination can occur when it has been determined that to do so would be in the best interest of the law enforcement/criminal justice community.

1. Exceptions:

   a. Road and weather data, which can be released to the public.

   b. Hazardous materials data can be given to fire departments, state board of health, and health care providers in emergency situations.

2. Missing person data in accordance with the 1982 Missing Children’s Act, which the IDACS Committee adopted on 10-02-1984. The Act stipulates that the user agencies can confirm entries on Unemancipated juveniles to parents, legal guardians and next of kin.

IV. User ID Requests

1. Requests for User ID’s should include a letter on department letterhead**,** a completed fingerprint card for each operator, a challenge question and answer for each operator and indicate if the operator is IDACS certified at another agency. The request must include the following:

   a. Name to include any aliases and maiden names.
   b. Date of Birth.
   c. Social Security Number.
   d. Results of III, CHRI, & Wanted File inquires (RF= Record Found, NR= No Record).
   e. Level of certification the operator will need to be assigned (Full, Inq, MDD).
   f. If operator is employed at more than one agency & also any past IDACS access operator has EVER held.

   g. If your agency has a system that interfaces with the IDACS switch (such as MDD & CAD systems) you must include the User ID/ LOGON assigned to your switch.

2. IDACS will assign ALL other User ID’s.

3. Once IDACS has assigned a User ID it cannot be changed. Marriages, divorces or any other legal name change will not affect or change the User ID.

4. Challenge questions must be submitted along with the fingerprint cards and request for a User ID. Challenge questions should be a personal question that only the operator can answer. The challenge question and answer must be in a separate sealed envelop enclosed with the above. If the challenge question is not properly completed, the request will be returned to the agency to be corrected.

5. A User ID may be requested to be disabled by a switched message to IDACS (INISP0007) or a letter requesting the User ID be disabled. The request must indicate if the user is IDACS certified at another agency.

V. Operator Background Policy and Procedures

1. In accordance with 240IAC 5-2-10, user agencies are required to guarantee the security clearance of all terminal and computer operators, including the submission of fingerprint cards to allow their background to be investigated.

2. The agency will assume full responsibility for all criminal history and wanted background checks for their agencies proposed IDACS operators. It is not the responsibility of the IDACS section to perform the checks or to obtain court document and final dispositions.

3. All terminal agencies must complete the following when requesting a User ID:

   a. Conduct a background check including but not limited to:
      1. Local criminal history check
      2. State criminal history check
      3. III criminal history check
      4. Inquire upon the following:
         a. Maiden names.
         b. Any name previously held
         c. Alias names.
         d. Additional DOB's or SSN's discovered in the background check.

4. When a record is discovered on a proposed operator a copy of the final disposition must be included with the proposed operator's information. The disposition will be reviewed and either approved or denied access by the Chairman of the IDACS Committee.

5. Forward along with the fingerprint card any criminal history records with disposition that is discovered.

6. Fingerprint Card Processing:

   a. The card must be properly filled out with all applicable descriptive data. If the fingerprint card is not properly filled out, the entire request will be returned to the agency to be corrected.

   b. The ORI block must show “INISP0000 CTR REC & ID-SPOL INDIANAPOLIS. IN.”

   c. The OCA block must contain the last seven (7) characters of your ORI ending with “IDX” (ex: 0520100IDX).

   d. The “EMPLOYER” block must show the complete name and address of the requesting agency.

   e. The reason fingerprinted block must contain: **“LAW ENFORCEMENT APPLICANT RE: IDACS/NCIC.”**

   f. Directions on the back of the card must be followed to insure good clear fingerprints.

   g. Once the card is processed by ISP Records and the FBI, and no criminal record is found, a letter from the FBI with the heading “Civil Applicant Response” will be sent to the submitting agency for filing and must be available for inspection by the IDACS Security Officer. FBI fingerprint cards will no longer be returned to the submitting agency, unless there is a criminal record or the fingerprints are deemed unclassifiable. Fingerprints deemed unclassifiable will be returned to the agency to be reprinted. If a copy of the fingerprint card is desired, the copy should be made by the agency prior to submitting to SP IDACS.

   h. If the ISP or FBI records check reveals a criminal history record, the fingerprint card will be returned to IDACS, who then will forward the card to the submitting agency for disposition.

   i. All criminal history record information will be forwarded to the IDACS Section for review. Once reviewed by the IDACS Committee Chairman, a determination will be made as to whether or not the person will be permitted to be an IDACS operator.

8. Regional Computer Center Agencies/ Agencies Accessing IDACS via a Computer Center Including Agencies with Mobile Data Devices (MDDs).

   a. The agency designated by the IDACS Committee as the Management Control Agency, will have the overall responsibility for the submission of the FBI applicant fingerprint card on all personnel connected with the Computer Center, i.e. data processing personnel as well as operators, and for agencies they service (this includes MDD agencies). Agencies served by the Center must submit a complete and accurate FBI applicant fingerprint card on each terminal operator to the Management Control Agency direct. Management Control Agencies of Computer Centers are given the option of retaining "Civil Applicant Response" for agencies that they service or returning those responses to the agency to be maintained.

b. Processing of cards by the Management Control Agency will include checking their local files, and then forwarding them to the State Police IDACS Section.

c. Any criminal record found must be brought to the attention of the IDACS Security Officer as soon as possible for further processing.

d. The Management Control Agency will be responsible for the assignment of User ID's to all operators of agencies served by the Computer Center.

e. Management Control Agencies will also be responsible for submitting to IDACS an alphabetical list of all persons fingerprinted by the 10th day of the even numbered months. This list must contain the NAME, User ID, and CERTIFICATION DUE DATE listing month, day, and year and be arranged according to agency.

VI. Quality Control

The following is information concerning quality control rules as listed in the Indiana Administrative Code (IAC).

1. Ten Minute Hit Procedures

a. Upon receipt of an urgent hit confirmation request from an inquiring agency, the originating agency (ORI) of the record must within ten (10) minutes, furnish a substantive response, i.e., a positive or negative confirmation or notice of the specific amount of time necessary to confirm or reject the record.

b. Upon receipt of a routine hit confirmation request, the originating agency (ORI) of record has up to one (1) hour to reply to the request.

c. It is the responsibility of the Coordinator to insure that all terminal operators utilize the Hit Confirmation Request and Response screen formats and follow the ten-minute hit procedures shown in the IDACS Manual.

VII. Responsibilities to Non-Terminal Agencies Serviced

1. Coordinators are to assist non-terminal agencies in their area that they service with any IDACS related issues.

a. Questions on security of IDACS/NCIC/NELTS data.

b. Keeping agencies informed of all available data through IDACS/NCIC/NLETS.

c. Informing new agency head of IDACS.

VIII. Where to Call for Assistance

1. SP IDACS Section

a. During normal business hours

1. Format questions and or problems.

2. Operational or administrative questions.

2. SP Data Operations Center (DOC)

a. Equipment Problems

1. Due to the wide range of terminal equipment now being used, IDACS or SP Data Operations Center **will not** be able to assist with equipment problems.

2. Prior to calling your vendor for service, check with Data Operations to determine if your terminal is acquired.

3. Contact your vendor for any hardware problems.

b. After Normal Business Hours

1. Operational or format questions.

2. Assist with expired passwords

3. IDACS Chairman or Area Representatives

a. Can be contacted concerning any questions on IDACS/NCIC/NLETS policies and procedures.

4. Regional Computer Centers

a. Agencies behind a regional computer center should contact the Regional Center Coordinator for any operational or equipment questions.

IX. IDACS Operator and Coordinator Certification Program

1. The following are training requirements as listed in the Indiana State Police Administrative Code (IAC).

240 IAC 5-2-11 IDACS Operator/Coordinator Certification Training

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 10-1-2.5-2

Sec. 11. (a) All IDACS terminal operators (including mobile terminals) shall be trained and tested for their proficiency at operating the IDACS terminal. All IDACS coordinators shall be trained and tested for their proficiency at operating the IDACS terminal and for their skills as the coordinator.

2. The objectives of training requirements shall be as follows:

a. To insure that coordinators and terminal operators are familiar with the laws governing IDACS/NCIC/NLETS, IDACS system rules, regulations, and procedures, and what files and functions are available and how to utilize them properly.

b. Create an awareness of IDACS/NCIC/NLETS System capabilities in order to allow criminal justice agencies to obtain maximum use of the system.

3. All persons assigned a User ID to operate the IDACS terminal and persons designated IDACS Coordinator by their agency shall be trained and tested according to the guidelines set forth by the IDACS Committee and approved by the State Police Superintendent.

4. Training course content is derived from the IDACS/NCIC/NLETS manuals and publications and will be periodically reviewed for relevancy, accuracy and updated accordingly.

5. The IDACS Committee can authorize the removal of a User ID, or impose sanctions on an agency for non-compliance with these procedures.

6. New terminal operators issued a User ID must be certified within the first six (6) months and re-certified every two years thereafter.

a. Coordinators must follow certification policies and regulations for scheduling operators for schools and test-outs.

b. Coordinators must be certified as an operator and within the first six (6) months of appointment be certified as Coordinator, re-certified every two years thereafter.

7. Requests for class attendance must be submitted in writing from the agency head to the IDACS Section.

a. Any changes or cancellations in attendance must be in writing and received prior to the first day of class.

X. IDACS User Agency Audits

1. IDACS User Agencies are periodically audited for compliance with rules, policies, and procedures.

a. Audits are conducted once every two years.

2. IDACS Audit Manual

a. Explanation in detail of what is reviewed during an audit.

XI. IDACS User Agency Sanctions

1. The following are sanction rules as listed in the Indiana Administrative Code (IAC). The IDACS sanctions policy is explained in Part 1 of the IDACS Manual.

240 IAC 5-2-12 User Agency Sanctions

Authority: IC 10-1-1-3; IC 10-1-2.5-7
Affected: IC 10-1-2.5-2

Sec. 12. (a) The IDACS Committee shall review violations of IDACS rules and make recommendations to the State Police Superintendent to impose sanctions on user agencies.

2. The objectives of the sanction procedure shall be as follows:

a. To insure the integrity of the System

b. Create an awareness among user agencies of the importance of following rules, regulations, and procedures in order to minimize the risk to liabilities that may be incurred by misuse of the SYSTEM and its data.

3. Sanctions shall be based upon the class of violation, any previous violations, and any exposure to criminal and civil liabilities that the violation might place on the SYSTEM, its' officials, and the offending agency.

4. Violations shall be classed as either Administrative (minor) or Security (serious) Violations. Security Violations are defined as one which has or could result in access of SYSTEM data by unauthorized individuals. All other violations are classed as Administrative.

5. In determining the severity of the Violation, the type, Administrative or Security, and if any previous sanctions issued, shall be considered. The IDACS Committee may impose sanctions by one of the following:

a. Verbal Warning

b. Written Warning

c. Written Notice of Violation

d. Written Notice of Probation

e. Written Notice of Temporary Suspension

f. Written Notice of Permanent Suspension

6. Temporary or permanent suspension of service will not begin, unless an emergency exists, until fifteen (15) days after the Agency Head has received written notice by certified mail or personal service.

7. An Agency may apply to be reinstated if placed on permanent suspension on or after (1) year.

8. The IDACS Committee shall review violations of IDACS rules and make recommendations to the State Police Superintendent to impose sanctions on user agencies.

9. The IDACS Committee may impose sanctions in accordance with item (e) above.

10. The definition of Suspension means: A definite time period for the termination of direct access to the IDACS system data as imposed by the IDACS Committee.

11. Upon receiving a written notice of violation(s), the user agency head shall submit in writing to the Chairman of the IDACS Committee any disciplinary action taken and/or procedures to correct the violation. This reply shall be within 30 days of the receipt of the notice of violation.

12. The user agency or IDACS Committee agency may cancel the user agency agreement with 30 days notice.